DIRETTIVA 2013/40/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 12 agosto 2013

relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 83, paragrafo 1,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo [1],

deliberando secondo la procedura legislativa ordinaria [2],

considerando quanto segue:

(1) Gli obiettivi della presente direttiva sono ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti, e migliorare la cooperazione fra le autorità competenti, compresi la polizia e gli altri servizi specializzati degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e il suo Centro europeo per la criminalità informatica, e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

(2) I sistemi di informazione sono un elemento chiave dell'interazione politica, sociale ed economica nell'Unione. La società è fortemente e sempre più dipendente da tali sistemi. Il buon funzionamento e la sicurezza di questi sistemi nell'Unione sono fondamentali per lo sviluppo del mercato interno e di un'economia competitiva e innovativa. La garanzia di un adeguato livello di protezione dei sistemi di informazione dovrebbe rientrare in un efficace quadro globale di misure di prevenzione a corredo delle risposte alla criminalità informatica nell'ambito del diritto penale.

(3) Gli attacchi ai danni dei sistemi di informazione, in particolare gli attacchi connessi alla criminalità organizzata, sono una minaccia crescente a livello di Unione e mondiale, e la preoccupazione per la possibilità di attacchi terroristici o di matrice politica contro sistemi di informazione che fanno parte dell'infrastruttura critica degli Stati membri e dell'Unione è in aumento. Ciò costituisce una minaccia per la creazione di una società dell'informazione più sicura e di uno spazio di libertà, sicurezza e giustizia, e richiede pertanto una risposta a livello di Unione, nonché un migliore coordinamento e una migliore cooperazione a livello internazionale.

(4) Vi sono nell'Unione infrastrutture critiche la cui distruzione o il cui danneggiamento avrebbe un significativo impatto transfrontaliero. Dalla necessità di rafforzare la capacità di protezione delle infrastrutture critiche nell'Unione risulta evidente che le misure contro gli attacchi informatici dovrebbero essere integrate con sanzioni penali rigorose che rispecchino la gravità di tali attacchi. Per infrastrutture critiche si potrebbe intendere un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico o sociale delle persone, come gli impianti energetici, le reti di trasporto o le reti governative, e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni.

(5) Si registra chiaramente una tendenza a perpetrare attacchi su larga scala sempre più pericolosi e ricorrenti contro sistemi di informazione che possono spesso essere critici per gli Stati membri o per particolari funzioni del settore pubblico o privato. Questa tendenza va di pari passo con lo sviluppo di metodi sempre più sofisticati, quali la creazione e l'uso delle cosiddette «botnet», che implica un reato costituito da più stadi, in cui ciascuno stadio singolarmente potrebbe mettere seriamente a rischio i pubblici interessi. La presente direttiva mira, tra l'altro, a introdurre sanzioni penali per la creazione delle «botnet», ossia per l'azione con cui si stabilisce il controllo a distanza di un numero rilevante di computer infettandoli con software maligni per mezzo di attacchi informatici mirati. Una volta creata, la rete infettata di computer che costituiscono la «botnet» può essere attivata a insaputa degli utenti per lanciare un attacco informatico su larga scala, che, solitamente, è in grado di causare danni gravi, ai sensi della presente direttiva. Gli Stati membri possono stabilire cosa costituisce danno grave ai sensi del loro diritto e della loro prassi nazionali, come ad esempio le perturbazioni dei servizi di sistema di rilevante interesse pubblico o la creazione di costi finanziari esorbitanti o la perdita di dati personali o di informazioni sensibili.

(6) Gli attacchi informatici su larga scala possono causare notevoli danni economici sia attraverso l'interruzione dei sistemi di informazione e delle comunicazioni sia attraverso la perdita o l'alterazione di informazioni riservate commercialmente importanti o di altri dati. Si dovrebbe prestare particolare attenzione alla sensibilizzazione delle piccole e medie imprese innovative con riguardo alle minacce relative a tali attacchi e alla loro vulnerabilità agli stessi, in conseguenza della loro crescente dipendenza dal corretto funzionamento e dalla disponibilità dei sistemi di informazione, e della disponibilità, spesso limitata, di risorse da dedicare alla sicurezza delle informazioni.

[1] GU C 218 del 23.7.2011, pag. 130.

[2] Posizione del Parlamento europeo del 4 luglio 2013 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 22 luglio 2013.

(7) Per garantire un approccio coerente degli Stati membri nell'applicazione della presente direttiva è importante disporre, in questo settore, di definizioni comuni.

(8) È necessario giungere a un approccio comune nei confronti degli elementi costitutivi dei reati mediante l'introduzione dei reati comuni di accesso illecito a sistemi di informazione, di interferenza illecita relativamente ai sistemi, di interferenza illecita relativamente ai dati e di intercettazione illecita.

(9) L'intercettazione comprende, ma non si limita necessariamente a, l'ascolto, il monitoraggio o la sorveglianza del contenuto di comunicazioni e il rilevamento del contenuto dei dati direttamente, mediante l'accesso e l'utilizzo dei sistemi di informazione, o indirettamente, mediante l'uso di dispositivi elettronici di intercettazione elettromagnetica o di intercettazione sulla linea tramite strumenti tecnici.

(10) Gli Stati membri dovrebbero prevedere sanzioni per gli attacchi ai danni di sistemi di informazione. Tali sanzioni dovrebbero essere effettive, proporzionate e dissuasive e comprendere pene detentive e/o pecuniarie.

(11) La presente direttiva prevede sanzioni penali almeno nei casi che non siano di minore gravità. Gli Stati membri possono stabilire cosa costituisce un caso di minore gravità ai sensi del loro diritto e della loro prassi nazionali. Un caso può essere considerato di minore gravità, ad esempio, qualora il danno causato dal reato e/o il rischio per gli interessi pubblici o privati, ad esempio per l'integrità di un sistema di informazione o per dati informatici, o per l'integrità, i diritti o altri interessi di una persona, sia insignificante o di natura tale da non rendere necessario imporre una sanzione penale entro i limiti di legge o stabilire una responsabilità penale.

(12) L'individuazione e la comunicazione di minacce e rischi posti dagli attacchi informatici, nonché la relativa vulnerabilità dei sistemi di informazione, costituiscono un elemento rilevante per un'efficace prevenzione e risposta agli attacchi informatici e del miglioramento della sicurezza dei sistemi di informazione. La previsione di incentivi per la segnalazione di lacune in materia di sicurezza potrebbe contribuire a tal fine. È opportuno che gli Stati membri si adoperino per rendere possibili l'individuazione legale e la segnalazione delle lacune in materia di sicurezza.

(13) È opportuno prevedere sanzioni più severe quando un attacco contro un sistema di informazione è perpetrato da un'organizzazione criminale quale definita nella decisione quadro 2008/841/GAI del Consiglio, del 24 ottobre 2008, relativa alla lotta contro la criminalità organizzata ([1]), quando un attacco informatico è condotto su larga scala, in tal modo colpendo un numero significativo di sistemi di informazione, anche quando è diretto alla creazione di una «botnet», o quando un attacco informatico causa danni gravi, anche nel caso in cui sia perpetrato attraverso una «botnet». È altresì opportuno prevedere sanzioni più severe quando un attacco è condotto contro un'infrastruttura critica degli Stati membri o dell'Unione.

(14) Altro elemento importante di un approccio intergrato alla criminalità informatica è l'istituzione di efficaci misure contro il furto d'identità e altri reati connessi all'identità. L'eventuale bisogno di un'azione dell'Unione contro tale tipo di comportamento criminale potrebbe anche essere considerato nel contesto di una valutazione della necessità di uno strumento orizzontale e globale dell'Unione.

(15) Nelle conclusioni del 27-28 novembre 2008, il Consiglio ha indicato che dovrebbe essere elaborata una nuova strategia con gli Stati membri e la Commissione, tenendo conto del contenuto della Convenzione del 2001 del Consiglio d'Europa sulla criminalità informatica. Tale Convenzione è il quadro giuridico di riferimento per la lotta contro la criminalità informatica, compresi gli attacchi contro i sistemi di informazione. La presente direttiva si basa su tale Convenzione. Il completamento del processo di ratifica di tale Convenzione il prima possibile da parte di tutti gli Stati membri dovrebbe essere considerata una priorità.

(16) Tenuto conto delle varie modalità con cui possono essere effettuati gli attacchi e della rapida evoluzione degli hardware e dei software, la presente direttiva fa riferimento a strumenti che possono essere utilizzati per commettere i reati in essa previsti. Tali strumenti potrebbero includere software maligni, fra cui quelli capaci di creare botnet, usati per perpetrare attacchi informatici. Anche se un tale strumento è idoneo o particolarmente idoneo a commettere i reati previsti nella presente direttiva, è possibile che sia stato prodotto per fini legittimi. Data la necessità di evitare una criminalizzazione di tali strumenti, quando essi siano prodotti e commercializzati per fini legittimi, come la verifica dell'affidabilità dei prodotti di tecnologia dell'informazione o la sicurezza dei sistemi di informazione, oltre al requisito dell'intenzione generale, deve essere soddisfatto anche il requisito dell'intenzione diretta di utilizzare tali strumenti per commettere uno o più reati previsti nella presente direttiva.

(17) La presente direttiva non prevede responsabilità penale qualora siano soddisfatti i criteri oggettivi dei reati previsti nella presente direttiva, ma gli atti siano compiuti senza dolo, ad esempio qualora una persona non sappia che l'accesso non è autorizzato o nel caso di incarichi di collaudo o di protezione di sistemi di informazione, ad esempio qualora una persona sia incaricata da un'impresa o da un venditore di verificare la resistenza del loro sistema di sicurezza. Nel contesto della presente direttiva, per gli obblighi o gli accordi contrattuali intesi a limitare l'accesso ai sistemi di informazione tramite norme d'uso o condizioni del servizio, nonché per controversie lavorative riguardo all'accesso e all'uso di sistemi di informazione di un datore di lavoro per scopi privati, non dovrebbe essere prevista responsabilità penale, quando l'accesso in tali circostanze sia ritenuto non autorizzato e, pertanto, costituisca l'unico presupposto per l'esercizio dell'azione penale. La presente direttiva non pregiudica il diritto di accesso alle informazioni, quale stabilito nel diritto nazionale e dell'Unione, ma al contempo non può costituire una giustificazione per l'accesso illecito o arbitrario alle informazioni.

([1]) GU L 300 dell'11.11.2008, pag. 42.

(18) Gli attacchi informatici potrebbero essere agevolati da svariate circostanze, come nel caso in cui l'autore del reato nell'ambito dell'esercizio della sua attività lavorativa abbia accesso ai sistemi di sicurezza connessi ai sistemi di informazione colpiti. È opportuno che, nel contesto del diritto nazionale, tali circostanze siano tenute in considerazione durante i procedimenti penali, ove opportuno.

(19) Gli Stati membri dovrebbero prevedere nel loro diritto nazionale circostanze aggravanti in conformità delle norme applicabili stabilite nei rispettivi ordinamenti giuridici in materia di circostanze aggravanti. Essi dovrebbero garantire che tali circostanze aggravanti possano essere tenute in conto dai giudici allorché giudicano gli autori di reati. La valutazione di tali circostanze, assieme agli altri elementi fattuali della singola fattispecie, resta discrezione del giudice.

(20) La presente direttiva non disciplina le condizioni per l'esercizio della competenza giurisdizionale su uno dei reati da essa contemplati, quali una querela della vittima nel luogo in cui il reato è stato commesso o una segnalazione dello Stato in cui è stato commesso, o il fatto che l'autore del reato non sia stato perseguito nel luogo in cui è stato commesso il reato.

(21) Nel contesto della presente direttiva gli Stati e gli organismi pubblici sono del tutto vincolati a garantire il rispetto dei diritti dell'uomo e delle libertà fondamentali, conformemente ai vigenti obblighi internazionali.

(22) La presente direttiva rafforza l'importanza delle reti, come la rete di punti di contatto del G8 o quella del Consiglio d'Europa, disponibili ventiquattr'ore su ventiquattro e sette giorni su sette. Tali punti di contatto dovrebbero poter prestare un'efficace assistenza, ad esempio agevolando lo scambio di pertinenti informazioni disponibili e la fornitura di consulenza tecnica o di informazioni giuridiche ai fini delle indagini o dei procedimenti relativi a reati connessi a sistemi di informazione e dati a essi associati che coinvolgono lo Stato membro richiedente. Per assicurare il buon funzionamento delle reti, ciascun punto di contatto dovrebbe essere in grado di comunicare con la massima urgenza con il punto di contatto di un altro Stato membro avvalendosi, tra l'altro, del supporto di personale addestrato e attrezzato. Data la rapidità con cui possono essere lanciati gli attacchi informatici su larga scala, gli Stati membri dovrebbero essere in grado di rispondere prontamente alle richieste urgenti provenienti da questa rete di punti di contatto. In casi siffatti può essere opportuno che la richiesta di informazioni, per garantirne la rapida evasione da parte dello Stato membro richiesto, sia accompagnata da un contatto telefonico e che i riscontri siano forniti entro otto ore.

(23) La cooperazione tra le autorità pubbliche da un lato, e il settore privato e la società civile dall'altro, è di grande importanza per prevenire e combattere gli attacchi contro i sistemi di informazione. È necessario promuovere e migliorare la cooperazione tra fornitori di servizi, produttori, organismi preposti all'applicazione della legge e autorità giudiziarie, nel pieno rispetto dello stato di diritto. Tale cooperazione potrebbe includere, ad esempio, l'assistenza da parte dei fornitori di servizi al fine di conservare possibili prove, fornire elementi che aiutino a identificare gli autori dei reati e, in ultima istanza, disattivare totalmente o parzialmente, conformemente al diritto e alla prassi nazionali, i sistemi di informazione o le funzioni che siano stati compromessi o utilizzati a fini illegali. Gli Stati membri dovrebbero altresì prendere in considerazione la creazione di reti di cooperazione e di partenariato con fornitori di servizi e produttori per lo scambio di informazioni relativamente ai reati che rientrano nell'ambito di applicazione della presente direttiva.

(24) È necessario raccogliere dati comparabili sui reati previsti nella presente direttiva. I dati pertinenti dovrebbero essere messi a disposizione delle agenzie e degli organismi specializzati dell'Unione, come Europol ed ENISA, in linea con le loro funzioni e necessità di informazione, per ottenere un quadro più completo del problema della criminalità informatica e della sicurezza delle reti e dell'informazione a livello di Unione e contribuire così alla formulazione di una risposta più efficace. Gli Stati membri dovrebbero trasmettere informazioni sul modus operandi degli autori dei reati a Europol e al suo Centro europeo per la lotta alla criminalità informatica ai fini dell'effettuazione di valutazioni delle minacce e di analisi strategiche in merito alla criminalità informatica conformemente alla decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di Polizia (Europol) [1]. La comunicazione di informazioni può agevolare una migliore comprensione delle minacce attuali e future, contribuendo così a una più idonea e mirata formulazione di decisioni sulla lotta e la prevenzione degli attacchi contro i sistemi di informazione.

(25) La Commissione dovrebbe presentare una relazione sull'applicazione della presente direttiva e formulare eventuali proposte legislative necessarie che potrebbero portare ad un ampliamento del suo ambito di applicazione, tenendo conto dell'evoluzione nell'ambito della criminalità informatica. Tale evoluzione potrebbe comprendere gli sviluppi tecnologici, ad esempio quelli che consentono un'applicazione più efficace della legge nel settore degli attacchi contro i sistemi di informazione o che facilitano la prevenzione di tali attacchi o la riduzione al minimo del loro impatto. A tal fine, la Commissione dovrebbe tenere conto delle analisi e delle relazioni disponibili, realizzate da attori pertinenti e, in particolare, da Europol e dall'ENISA.

(26) Al fine di combattere efficacemente la criminalità informatica, è necessario aumentare la resilienza dei sistemi di informazione, adottando le misure adeguate per proteggerli in modo più efficace contro gli attacchi informatici. Gli Stati membri dovrebbero adottare le misure necessarie per proteggere le loro infrastrutture critiche dagli attacchi informatici e in tale ambito dovrebbero prendere in considerazione la protezione dei loro sistemi di

[1] GU L 121 del 15.5.2009, pag. 37.

informazione e dei dati associati. Costituisce parte essenziale di un approccio globale a una lotta efficace contro la criminalità informatica assicurare un adeguato livello di protezione e di sicurezza dei sistemi di informazione a opera di persone giuridiche, ad esempio in relazione ai servizi di comunicazione elettronica di pubblico accesso, conformemente alla vigente legislazione dell'Unione in materia di vita privata e comunicazioni elettroniche e protezione dei dati. Dovrebbero essere forniti livelli di protezione adeguati contro le minacce e le vulnerabilità ragionevolmente individuabili in maniera corrispondente allo stato dell'arte degli specifici settori e alle specifiche situazioni di trattamento dei dati. Il costo e l'onere di tale protezione dovrebbero essere commisurati al danno potenziale procurato da un attacco informatico ai soggetti interessati. Gli Stati membri sono incoraggiati a prevedere, nell'ambito del loro diritto nazionale, pertinenti misure per l'attribuzione di responsabilità per i casi un cui una persona giuridica non abbia manifestamente fornito un adeguato livello di protezione contro gli attacchi informatici.

(27) Le rilevanti lacune e le notevoli differenze nel diritto e nelle procedure penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione possono ostacolare la lotta contro la criminalità organizzata e il terrorismo e possono complicare un'efficace cooperazione di polizia e giudiziaria in questo settore. Il carattere transnazionale e senza frontiere dei moderni sistemi di informazione fa sì che gli attacchi contro tali sistemi abbiano una dimensione transfrontaliera, e rende evidente la necessità urgente di adottare azioni ulteriori per il ravvicinamento del diritto penale in questo settore. L'attuazione e l'applicazione adeguate della decisione quadro 2009/948/GAI del Consiglio, del 30 novembre 2009, sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali ([1]), dovrebbero inoltre agevolare il coordinamento dell'azione penale nei casi di attacchi contro i sistemi di informazione. Gli Stati membri, in collaborazione con l'Unione, dovrebbero altresì cercare di migliorare la cooperazione internazionale relativamente alla sicurezza dei sistemi di informazione, delle reti informatiche e dei dati informatici. Qualsiasi accordo internazionale riguardante lo scambio di dati dovrebbe tenere debito conto della sicurezza del trasferimento e dello stoccaggio dei dati.

(28) Una migliore cooperazione tra competenti organismi preposti all'applicazione della legge e autorità giudiziarie in tutta l'Unione è essenziale ai fini di una lotta efficace contro la criminalità informatica. In tale contesto, si dovrebbe incoraggiare l'intensificazione degli sforzi, intesi a fornire una formazione adeguata alle pertinenti autorità, al fine di aumentare la comprensione della criminalità informatica e del suo impatto e promuovere la cooperazione e lo scambio di migliori pratiche, ad esempio attraverso le competenti agenzie e organismi specializzati dell'Unione. Tale formazione dovrebbe mirare, tra l'altro, ad aumentare il grado di conoscenza dei diversi ordinamenti giuridici nazionali, delle possibili sfide giuridiche e tecniche da affrontare nelle indagini penali e della ripartizione delle competenze tra le competenti autorità nazionali.

(29) La presente direttiva rispetta i diritti umani e le libertà fondamentali e osserva i principi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea e dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, inclusi la protezione dei dati personali, il diritto alla riservatezza, la libertà di espressione e d'informazione, il diritto a un processo equo, la presunzione di innocenza e i diritti della difesa così come i principi della legalità e della proporzionalità dei reati e delle pene. In particolare, la presente direttiva è volta a garantire il pieno rispetto di tali diritti e principi e deve essere attuata di conseguenza.

(30) La protezione dei dati personali costituisce un diritto fondamentale conformemente all'articolo 16, paragrafo 1, TFUE e all'articolo 8 della Carta dei diritti fondamentali. Pertanto, qualsiasi trattamento di dati personali nell'ambito dell'attuazione della presente direttiva dovrebbe avvenire nel pieno rispetto del pertinente diritto dell'Unione in materia di protezione dei dati.

(31) A norma dell'articolo 3 del protocollo sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, detti Stati membri hanno notificato che desiderano partecipare all'adozione e all'applicazione della presente direttiva.

(32) A norma degli articoli 1 e 2 del protocollo sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione della presente direttiva, non è da essa vincolata né è soggetta alla sua applicazione.

(33) Poiché gli obiettivi della presente direttiva, segnatamente assoggettare gli attacchi ai danni di sistemi di informazione in tutti gli Stati membri a sanzioni penali effettive, proporzionate e dissuasive, e migliorare e incoraggiare la cooperazione giudiziaria, non possono essere conseguiti in misura sufficiente dagli Stati membri, e possono dunque, a motivo della loro portata o dei loro effetti, essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(34) La presente direttiva mira a modificare e ampliare le disposizioni della decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione ([2]). Poiché le modifiche da apportare sono sostanziali per numero e natura, a fini di chiarezza, è opportuno che la decisione quadro 2005/222/GAI sia integralmente sostituita per gli Stati membri che partecipano all'adozione della presente direttiva,

([1]) GU L 328 del 15.12.2009, pag. 42.

([2]) GU L 69 del 16.3.2005, pag. 67.

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

Articolo 1

Oggetto

La presente direttiva stabilisce norme minime per la definizione dei reati e delle sanzioni nel settore degli attacchi contro i sistemi di informazione. Essa mira inoltre a facilitare la prevenzione di tali reati e a migliorare la cooperazione tra autorità giudiziarie e altre autorità competenti.

Articolo 2

Definizioni

Ai fini della presente direttiva s'intende per:

a) «sistema di informazione»: un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione;

b) «dati informatici»: una rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata in un sistema di informazione, compreso un programma atto a far svolgere una funzione a un sistema di informazione;

c) «persona giuridica»: un'entità che ha lo status di persona giuridica in forza del diritto applicabile; la definizione non include gli Stati o gli organismi pubblici che agiscono nell'esercizio dell'autorità statale o le organizzazioni pubbliche internazionali;

d) «senza diritto»: una condotta di cui alla presente direttiva, ivi inclusi l'accesso, l'interferenza o l'intercettazione, che non è autorizzata da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentiti a norma del diritto nazionale.

Articolo 3

Accesso illecito a sistemi di informazione

Gli Stati membri adottano le misure necessarie per garantire che, se intenzionale, l'accesso senza diritto a un sistema di informazione o a una parte dello stesso, sia punibile come reato qualora sia commesso in violazione di una misura di sicurezza, almeno per i casi che non sono di minore gravità.

Articolo 4

Interferenza illecita relativamente ai sistemi

Gli Stati membri adottano le misure necessarie a garantire che l'atto di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati o rendendo tali dati inaccessibili, compiuto intenzionalmente e senza diritto, sia punito come reato almeno per i casi che non sono di minore gravità.

Articolo 5

Interferenza illecita relativamente ai dati

Gli Stati membri adottano le misure necessarie a garantire che l'atto di cancellare, danneggiare, deteriorare, alterare, sopprimere dati informatici in un sistema di informazione, o di rendere tali dati inaccessibili, compiuto intenzionalmente e senza diritto, sia punibile come reato, almeno per i casi che non sono di minore gravità.

Articolo 6

Intercettazione illecita

Gli Stati membri adottano le misure necessarie affinché l'intercettazione, tramite strumenti tecnici, di trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici, compiuta intenzionalmente e senza diritto, sia punibile come reato, almeno per i casi che non sono di minore gravità.

Articolo 7

Strumenti utilizzati per commettere i reati

Gli Stati membri adottano le misure necessarie affinché la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo intenzionali di uno dei seguenti strumenti, compiuti senza diritto e con l'intenzione di utilizzarli al fine di commettere uno dei reati di cui agli articoli da 3 a 6, siano punibili come reato, almeno per i casi che non sono di minore gravità:

a) un programma per computer, destinato o modificato principalmente al fine di commettere uno dei reati di cui agli articoli da 3 a 6;

b) una password di un computer, un codice d'accesso, o dati simili che permettono di accedere in tutto o in parte a un sistema di informazione.

Articolo 8

Istigazione, favoreggiamento, concorso e tentativo

1. Gli Stati membri garantiscono che l'istigazione o il favoreggiamento e il concorso nella commissione di un reato di cui agli articoli da 3 a 7 siano punibili come reato.

2. Gli Stati membri garantiscono che il tentativo di commettere un reato di cui agli articoli 4 e 5 sia punibile come reato.

Articolo 9

Sanzioni

1. Gli Stati membri adottano le misure necessarie ad assicurare che i reati di cui agli articoli da 3 a 8 siano punibili con sanzioni effettive, proporzionate e dissuasive.

2. Gli Stati membri adottano le misure necessarie ad assicurare che i reati di cui agli articoli da 3 a 7 siano punibili con una pena detentiva massima non inferiore a due anni, almeno per i casi che non sono di minore gravità.

3. Gli Stati membri adottano le misure necessarie ad assicurare che i reati di cui agli articoli 4 e 5, se commessi intenzionalmente, siano punibili con una pena detentiva massima non

inferiore a tre anni, se un numero significativo di sistemi di informazione è stato colpito avvalendosi di uno degli strumenti di cui all'articolo 7, destinato o modificato principalmente a tal fine.

4. Gli Stati membri adottano le misure necessarie ad assicurare che i reati di cui agli articoli 4 e 5 siano punibili con una pena detentiva massima non inferiore a cinque anni, qualora:

a) siano commessi nell'ambito di un'organizzazione criminale quale definita nella decisione quadro 2008/841/GAI, indipendentemente dalla sanzione ivi prevista;

b) causino danni gravi; o

c) siano commessi ai danni di un sistema di informazione di un'infrastruttura critica.

5. Gli Stati membri adottano le misure necessarie ad assicurare che, qualora i reati di cui agli articoli 4 e 5 siano commessi abusando dei dati personali di un'altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al legittimo proprietario dell'identità, ciò possa, conformemente al diritto nazionale, essere considerato una circostanza aggravante, purché tale circostanza non sia già contemplata da un altro reato punibile a norma del diritto nazionale.

Articolo 10

Responsabilità delle persone giuridiche

1. Gli Stati membri adottano le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili dei reati di cui agli articoli da 3 a 8, commessi a loro vantaggio da qualsiasi persona, che agisca a titolo individuale o in quanto membro di un organismo della persona giuridica, e che detenga una posizione dominante in seno alla persona giuridica basata:

a) sul potere di rappresentanza della persona giuridica;

b) sul potere di prendere decisioni per conto della persona giuridica;

c) sul potere di esercitare il controllo in seno alla persona giuridica.

2. Gli Stati membri adottano le misure necessarie ad assicurare che le persone giuridiche possano essere ritenute responsabili qualora la mancata sorveglianza o il mancato controllo da parte di una persona di cui al paragrafo 1 abbia permesso la commissione, da parte di una persona sotto la sua autorità, di uno dei reati di cui agli articoli da 3 a 8 a vantaggio di tale persona giuridica.

3. La responsabilità delle persone giuridiche a norma dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che siano autori o istigatori o abbiano concorso in uno dei reati di cui agli articoli da 3 a 8.

Articolo 11

Sanzioni applicabili alle persone giuridiche

1. Gli Stati membri adottano le misure necessarie ad assicurare che una persona giuridica ritenuta responsabile a norma dell'articolo 10, paragrafo 1, sia punibile con sanzioni effettive, proporzionate e dissuasive, che comprendano sanzioni pecuniarie penali o non penali e che possano comprendere altre sanzioni, quali:

a) l'esclusione dal godimento di un beneficio o aiuto pubblico;

b) l'interdizione temporanea o permanente dall'esercizio di attività commerciali;

c) l'assoggettamento a sorveglianza giudiziaria;

d) provvedimenti giudiziari di scioglimento;

e) la chiusura temporanea o permanente degli stabilimenti che sono stati usati per commettere il reato.

2. Gli Stati membri adottano le misure necessarie ad assicurare che una persona giuridica ritenuta responsabile a norma dell'articolo 10, paragrafo 2, sia punibile con sanzioni o altre misure effettive, proporzionate e dissuasive.

Articolo 12

Competenza giurisdizionale

1. Gli Stati membri stabiliscono la propria competenza giurisdizionale relativamente ai reati di cui agli articoli da 3 a 8 quando il reato sia stato commesso:

a) in tutto o in parte sul loro territorio; o

b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso.

2. Nello stabilire la propria competenza giurisdizionale conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora:

a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o

b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato.

3. Uno Stato membro informa la Commissione ove decida di stabilire la competenza giurisdizionale per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora:

a) l'autore del reato risieda abitualmente nel suo territorio; o

b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio.

Articolo 13

Scambio di informazioni

1. Per lo scambio di informazioni relative ai reati di cui agli articoli da 3 a 8, gli Stati membri garantiscono di predisporre un punto di contatto operativo nazionale e di utilizzare la rete esistente di punti di contatto operativi disponibili ventiquattr'ore su ventiquattro e sette giorni su sette. Gli Stati membri garantiscono inoltre di predisporre procedure tali da consentire all'autorità competente, in caso di richieste urgenti di assistenza, di indicare, entro otto ore dalla richiesta, almeno se la richiesta sarà soddisfatta e la forma e il tempo stimato per tale risposta.

2. Gli Stati membri informano la Commissione in merito al proprio punto di contatto di cui al paragrafo 1. La Commissione trasmette tali informazioni agli altri Stati membri e alle competenti agenzie e organismi specializzati dell'Unione.

3. Gli Stati membri adottano le misure necessarie ad assicurare che siano disponibili idonei canali di comunicazione per agevolare le comunicazioni alle autorità nazionali competenti sui reati di cui all'articolo da 3 a 6 senza indebito ritardo.

Articolo 14

Monitoraggio e statistiche

1. Gli Stati membri provvedono a predisporre un sistema di registrazione, produzione e fornitura di dati statistici sui reati di cui agli articoli da 3 a 7.

2. I dati statistici di cui al paragrafo 1 riguardano come minimo i dati esistenti sul numero dei reati di cui agli articoli da 3 a 7 registrati dagli Stati membri e il numero di persone che sono state oggetto di un procedimento giudiziario e che sono state condannate per i reati di cui agli articoli da 3 a 7.

3. Gli Stati membri trasmettono alla Commissione i dati raccolti a norma del presente articolo. La Commissione provvede alla pubblicazione di una revisione consolidata delle relazioni statistiche e a trasmetterla alle competenti agenzie e organismi specializzati dell'Unione.

Articolo 15

Sostituzione della decisione quadro 2005/222/GAI

La decisione quadro 2005/222/GAI è sostituita in relazione agli Stati membri che partecipano all'adozione della presente direttiva, fatti salvi gli obblighi degli Stati membri relativi al termine per il recepimento della decisione quadro nel diritto nazionale.

In relazione agli Stati membri che partecipano all'adozione della presente direttiva, i riferimenti alla decisione quadro 2005/222/GAI si intendono fatti alla presente direttiva.

Articolo 16

Recepimento

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 4 settembre 2015.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni che recepiscono nei rispettivi diritti nazionali gli obblighi imposti dalla presente direttiva.

3. Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

Articolo 17

Relazione

Entro il 4 settembre 2017 la Commissione presenta al Parlamento europeo e al Consiglio una relazione che valuta in quale misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla presente direttiva, corredata, se del caso, di proposte legislative. La Commissione tiene altresì conto degli sviluppi tecnici e giuridici in materia di criminalità informatica, con particolare riguardo all'ambito di applicazione della presente direttiva.

Articolo 18

Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 19

Destinatari

Gli Stati membri sono destinatari della presente direttiva conformemente ai trattati.

Fatto a Bruxelles, il 12 agosto 2013

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
M. SCHULZ	L. LINKEVIČIUS